1972

Some lattice theoretic theorems concerning the submodules of a module.

Jensen, Gary Dean.

University of Texas at Austin

SOME LATTICE THEORETIC THEOREMS CONCERNING THE SUBMODULES OF A MODULE

Gary Dean Jensen

SOME LATTICE THEORETIC THEOREMS CONCERNING

THE TOPOLOGY OF A MODULE

APPROVED:

____

____

SOME LATTICE THEORETIC THEOREMS CONCERNING THE SUBMODULES OF A MODULE

SOME LATTICE THEORETIC THEOREMS CONCERNING THE SUBMODULES OF A MODULE

by

GARY DEAN JENSEN, B.S.

THESIS

Presented to the Faculty of the Graduate School of

The University of Texas at Austin

in Partial Fulfillment

of the Requirements

for the Degree of

MASTER OF ARTS

THE UNIVERSITY OF TEXAS AT AUSTIN

August 1972

PREFACE

The purpose of this paper is to investigate certain properties of the lattice of submodules of a module.

Primary attention is given to what restrictions must be placed on the module in order to insure that the lattice structure will have distributivity or complementation. In general, these restrictions are placed on the ring of scalars of the module, though in certain cases other requirements are necessary also.

In Section I, the set of all submodules of a module is shown to be a lattice and meets and joins are characterized in this lattice. It is established that this lattice is always modular. In Section II, it is shown under what conditions the lattice of submodules will be distributive. In arriving at the theorems of this section, much reference was made to work by O. Ore on this same problem with groups and subgroups. Section III deals with what conditions are sufficient to insure that the lattice of submodules is complemented. Section IV makes brief comments about covering properties in the lattice of submodules.

In this paper, a basic knowledge of module theory and lattice theory is assumed. All rings are assumed to possess a unit element, and all modules are considered as left R-modules.

In general, the notation used is that of MacLane and Birkhoff in Algebra, particularly the use of "$\wedge$" for meets and "$\vee$" for joins of elements in a lattice. The notion of a distributive pair and the notation, D-R-module, is adopted from the paper by O. Ore on the lattice structure of subgroups. If $c \in M$, the submodule of M, generated by c, will be denoted by [c]. In the manner of Kaplansky and others, theorems have been numbered consecutively throughout the paper.

C O N T E N T S

SECTION 1. CHARACTERIZATION OF $L_R(M)$.

In this section, it is established that the lattice of all R-submodules of an R-module is a modular lattice and its lattice operations are characterized. Throughout, it will be assumed that R is a ring and that M is an R-module.

DEFINITION. $L_R(M)=\{A \mid A$ is R-submodule of M$\}$. For $A, B \in L_R(M)$, $A \leq B$ shall mean $A \subseteq B$.

The fact that $(L_R(M), \leq)$ is a lattice will follow from the following well-known theorem.

THEOREM I. *Let $(P,\leq)$ be a poset. If $(P,\leq)$ has a largest element and has the property that if $\mathcal{S} \subseteq P$ and $\mathcal{S} \neq \emptyset$, then the infinum of $\mathcal{S}$ exists in $(P,\leq)$, then $(P,\leq)$ is a complete lattice.*[1]

THEOREM II. *If M is any R-module, and $L_R(M)$ is the set of all submodules of M, ordered by set inclusion, then*

---

[1] G. Szasz, *Introduction to Lattice Theory* (3d ed. New York and London: Academic Press, 1963), p. 61.

i) $\underline{L_R(M) \text{ is a complete lattice}}$

iii) $\underline{\{0\} \text{ is the null element of } L_R(M)}$

iii) $\underline{M \text{ is the unit element of } L_R(M)}$

iv) $\underline{\text{If } A_\alpha \in L_R(M) \text{ for every } \alpha\in\Gamma \text{ then } \bigwedge_{\alpha\in\Gamma} A = \bigcap_{\alpha\in\Gamma} A}$

v) $\underline{\text{If } A,B \in L_R(M) \text{ then } A \vee B = A + B}$

vi) $\underline{\text{If } A_\alpha \in L_R(M) \text{ for every } \alpha \in \Gamma \text{ then }} \bigvee_{\alpha\in\Gamma} A_\alpha = \{x \in M|$ $\underline{\text{there exist } \alpha_1, \alpha_2, \ldots, \alpha_n \in \Gamma, \text{ and}}$ $\underline{a_1, a_2, \ldots, a_n \text{ such that } a_i \in A_{\alpha_i} \text{ for}}$ $\underline{\text{every } i \text{ and } x = a_1 + a_2 + \ldots + a_n}\}$

<u>Proof</u>. Clearly $(L_R(M),\leq)$ is a partially ordered set. Further, M is the largest element of $L_R(M)$. If $\mathcal{S}$ is an non-empty subfamily of $L_R(M)$, $\bigcap_{S\in\mathcal{S}} S$ is a submodule of M which serves as the inf in the $\leq$ order of $L_R(M)$. Thus $(L_R(M),\leq)$ is a complete lattice with unit element M and lattice meets characterized by set intersection.

Clearly A+B is a submodule of M, containing A and B, and contained in every submodule containing both A and B; therefore, $A\vee B=A+B$. More generally, if Γ is an index set and $A \in L_R(M)$ for each $\alpha\in\Gamma$, let

$$B = \{x \in M| \text{ there exist } \alpha_1, \ldots, \alpha_n \in \Gamma \text{ and } a_1, \ldots, a_n \in M \text{ such that } a_i \in A_{\alpha_i} \text{ for each } i \text{ and } x = a_1+a_2+\ldots+a_n\};$$

then B is a submodule of M such that $A \leq B$ for each $\alpha \in \Gamma$.

Furthermore, if C is a submodule such that $A_\alpha \leq C$ for each $\alpha\in\Gamma$, then $C \leq B$. Thus $B = \bigvee_{\alpha\in\Gamma} A_\alpha$.

$\{0\}$ is immediately a submodule which is a subset of each submodule.

Now, the natural question arises: what properties does $L_R(M)$ have, and in what way are these properties dependent upon our choice of M

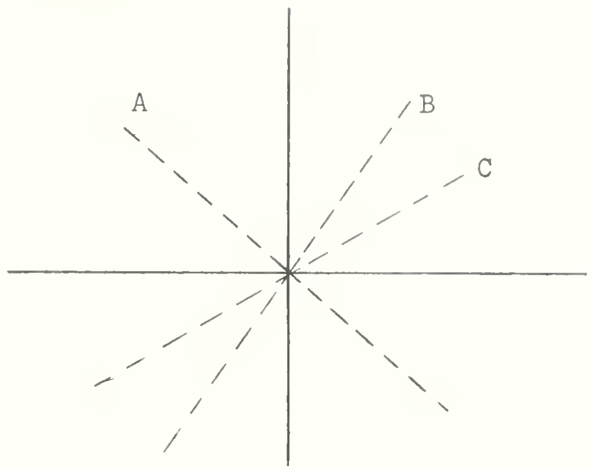
First, consider a property of $L_R(M)$ that is independent of M.

THEOREM III. $L_R(M)$ is modular.

Proof. To show $L_R(M)$ modular, we need to show that for $A, B, C \in L_R(M)$, $A \geq B$ implies $A\wedge(B\vee C) = B\vee(A\wedge C)$. Since $B\vee(A\wedge C) \leq A\wedge(B\vee C)$ is valid in any lattice, we need only show $B\vee(A\wedge C) \geq A\wedge(B\vee C)$. Now $x \in A\wedge(B\vee C)$ implies $x \in A$, $x \in (B\vee C)$ so $x = b + c$, $b \in B$, $c \in C$. $A \geq B$, $b \in B$ implies $b \in A$ so $-b \in A$. Thus $x \in A$, $-b \in A$ and $-b + x \in A$. Then $-b + x = -b + b + c = c \in A$; hence $c \in A$ and $c \in C$ which implies $c \in A\wedge C$. Thus $x = b + c$ where $b \in B$, $c \in (A\wedge C)$ so $x \in B\vee(A\wedge C)$ and $B\vee(A\wedge C) \geq A\wedge(B\vee C)$. Therefore the modular equality holds, so $L_R(M)$ is modular.

The stronger statement that $L_R(M)$ is distributive is not, in general, true.

<u>EXAMPLE</u>. Consider two dimensional vector space over the ring R of real numbers. Since this is a vector space, it is a module.



Any line through the origin would be a subspace; therefore, a submodule. However, $A \wedge (B \vee C)$ for A, B, C, as indicated in the sketch, is just A, since $B \vee C = B + C$ the entire plane. But $(A \wedge B) \vee (B \wedge C) = \{0\}$, the null element of the lattice. Thus, for this case $L_R(M)$ is not distributive.

While it is true that $L_R(M)$ is not always distributive, there are certain interesting classes where $L_R(M)$ is distributive. For example, the ring of integers as a module over itself is distributive.

Thus, it is interesting to note what restriction must be placed on M in order that $L_R(M)$ be distributive. This problem will be studied in the next section.

SECTION 2. DISTRIBUTIVITY CONDITION.

This section characterizes when $L_R(M)$ will be distributive under the assumption that the ring R is a principal ideal domain. The results of this section are an adaptation of Ore's paper on subgroups of a group.[1] In order to arrive at the main theorem of this section, some preliminary definitions and a lemma are necessary.

DEFINITION. A pair (A, B) of submodules A and B of a module M is said to be a distributive pair if the distributive law

$$C \wedge (A \vee B) = (C \wedge A) \vee (C \wedge B)$$

holds for every submodule C of M.

Now let R be a principal ideal domain, and M be an R-module. If x is an element of M, and A a submodule of M, consider the set

$$X_A = \{r \in R: \quad rx \in A\}$$

X_A is an ideal since:

i) $0x = 0 \in A$ so X_A is nonempty.

ii) $r \in X_A$, $s \in X_A$ then $r + s \in X_A$.

iii) $r \in X_A$ then $hr \in X_A$ for every $h \in R$.

---

[1] O. Ore, Structures and group theory, II. Duke Math. J. 4 (1938), pp. 267-268.

R is a principal ideal domain so there exists a generator of X_A.

<u>Remark</u>. The divides relation and the highest common factor properties of a principal ideal ring will be used without proof throughout this section.

<u>DEFINITION</u>. If $X_A \neq \{0\}$, then there exists an element $r_A \in R$ such that r_A generates X_A. r_A is said to be the <u>relative order</u> of x with respect to A, and it is said the relative order of x with respect to A is <u>finite</u>.

<u>LEMMA 1</u>. <u>Given R a principal ideal domain and M an R-module, A,B submodules of M. Then A and B form a distributive pair if and only if for every element c of $A \vee B$, c not in A or B the relative orders of c with respect to A and B are finite and relatively prime to each other</u>.

<u>Proof</u>. Suppose that a pair (A,B) is distributive. If an element of $A \vee B$ is contained in neither A nor B, then

$$C = [c] = C \wedge (A \vee B) = (C \wedge A) \vee (C \wedge B)$$

by the distributivity of the pair A,B. Moreover, neither $(C \wedge A)$ nor $(C \wedge B)$ is equal to $\{0\}$ since then

$$(C \wedge A) \vee (C \wedge B) = (C \wedge B) = C$$

which implies $c \in B$ which is a contradiction.

Now since $(C \wedge A) = C_A c = \{rc | r \in C_A\} \neq \{0\}$ implies $C_A \neq \{0\}$ and similarly for $(C \wedge B)$ and C_B, the relative orders r_A and r_B are finite.

Now if r_A generates C_A, then $r_A c$ generates $(C \wedge A)$ and likewise $r_B c$ generates $(C \wedge B)$ then $C = [c] = (C \wedge A) \vee (C \wedge B)$ implies $[c] = [r_A c]\ [r_B c]$ and therefore $c = xr_A c + yr_B c = (xr_A + yr_B)c$.

Therefore, $(xr_A + yr_B - 1) \in$ order c. Since order $c = \{r \in R | rc = 0\}$, which is an ideal hence principal, let n generate order c. Now $nc = 0 \in A$ so $n \in C_A$ and $n = wr_A$. Therefore, $xr_A + yr_B - 1 = zn = zwr_A$, where $z \in R$. Hence $(x - zw)r_A + yr_B = 1$ and thus we have r_A and r_B relatively prime.

To establish the converse, it will first be shown that every submodule C of $A \vee B$ is a join of $(C \wedge A)$ and $(C \wedge B)$. This then will insure the distributivity of the pair (A, B). If $C \subseteq A \vee B$, then clearly $(C \wedge A) \vee (C \wedge B) \subseteq C$. Thus it need only be shown that every $c \in C$ is an element of $(C \wedge A) \vee (C \wedge B)$.

If $c \in (C \wedge A)$ or $c \in (C \wedge B)$, it is immediate. If $c \notin (C \wedge A)$ and $c \notin (C \wedge B)$, then by assumption the orders of c with respect to $(C \wedge A)$ and $(C \wedge B)$ are finite and relatively prime. Let r_A be the relative order of c with respect to $(C \wedge A)$, r_B the relative order of c with respect to $(C \wedge B)$. Then $r_A c \in (C \wedge A)$ and $r_B c \in (C \wedge B)$.

By assumption, r_A and r_B are relatively prime; hence there exists $x, y \in R$ such that $xr_A + yr_B = 1$. Then

$$c = 1 \cdot c = (xr_A + yr_B)c = xr_Ac + yr_Bc.$$

Since $(C \wedge A)$ and $(C \wedge B)$ are submodules, $r_Ac \in (C \wedge A)$ implies $xr_Ac \in (C \wedge A)$ and $r_Bc \in (C \wedge B)$ implies $yr_Bc \in (C \wedge B)$. Thus $c = a + b$ where $xr_Ac = a \in (C \wedge A)$, $yr_Bc = b \in (C \wedge B)$ so $C = (C \wedge A) \vee (C \wedge B)$.

Now for arbitrary C, $C \wedge (A \vee B)$ is a submodule of $(A \vee B)$ so $C \wedge (A \vee B)$ is the join of $C \wedge (A \vee B) \wedge A = C \wedge A$ and $C \wedge (A \vee B) \wedge B = C \wedge B$, thus $C \wedge (A \vee B) = (C \wedge A) \vee (C \wedge B)$ for every submodule C and therefore (A, B) is a distributive pair.

DEFINITION. An R-module M is a D-R-module if its $L_R(M)$ lattice is distributive.

With the help of the preceding definitions and the lemma, the following theorem may now be stated and proved.

THEOREM IV. *Let R be a principal ideal domain and M an R-module. Then M is a D-R-module if and only if every finite set of elements of M generates a cyclic submodule.*

Proof: To show sufficiency first, assume every finite set of elements generates a cyclic submodule. It will be

established that each pair (A,B) of submodules is a distributive pair. This will be done if for every element c, $c \in A \vee B$ with $c \notin A$ and $c \notin B$, the relative orders of c with respect to A and to B are relatively prime, since then by the lemma, (A,B) will be a distributive pair.

Consider such a pair, (A,B) and an element $c \in A \vee B$ such that $c \notin A$, $c \notin B$. Then $c = a + b$ where $a \in A$ and $b \in B$. Now the elements $a,b \in M$ generate the submodule $Ra + Rb$, so by assumption, $Ra + Rb$ must be cyclic. Thus there exists an element $g \in M$ such that $Rg = Ra + Rb$. Then $a \in Ra + Rb$ implies there exists $r_1 \in R$ such that $r_1 g = a$. Similarly, there exists an $r_2 \in R$ such that $r_2 g = b$. Now g can be chosen in such a way that r_1 and r_2 are relatively prime. Consider (r_1, r_2), if it equals 1, then obviously no proof is needed. If it is not equal to 1, then there exists $n,m \in R$ such that $(r_1,r_2)n = r_1$ and $(r_1,r_2)m = r_2$. Now $r_1 \neq 0$ and $r_2 \neq 0$ since $r_1 = 0$ implies $r_1 g = a = 0$ so $c = a + b = 0 + b$ and $c \in B$, but this is a contradiction since c was chosen so that $c \notin B$. Similarly $r_2 = 0$ implies $c \in A$ which is also a contradiction, so we have $r_1 \neq 0$, $r_2 \neq 0$. Then $(n,m) = 1$ and $(r_1,r_2)ng = r_1 g = a$ and $(r_1,r_2)mg = r_2 g = b$. If $g' = (r_1,r_2)g$, then $ng' = a$ and $mg' = b$; and $Rg' = Ra + Rb$ since $Rg' \subseteq Rg = Ra + Rb$

and $a, b \in Rg'$ implies $Ra + Rb \subseteq Rg'$. Thus there exists a g' such that $Rg' = Ra + Rb$ and $ng' = a$, $mg' = b$, where $(n,m) = 1$. So $Rg = Ra + Rb$ where $r_1 g = a$, $r_2 g = b$ and r_1, r_2 are relatively prime. Now $c = a + b$ so $r_1 c = r_1 a + r_1 b$ but $b = r_2 g$ so $r_1 c = r_1 a + r_1 r_2 g$. Since R is commutative, $r_1 c = r_1 a + r_2(r_1 g) = (r_1 a + r_2 a) \in A$; therefore, $r_1 c \in A$ and $r_1 \in C_A$. Thus $C_A \neq \{0\}$, so if r_A is the order of c with respect to A, r_A is finite. Then $r_1 \in C_A$ implies $r_A | r_1$. Similarly $r_2 c \in B$ and r_B, the relative order of c with respect to B, divides r_2. Thus $(r_A, r_B) | r_1$ and $(r_A, r_B) | r_2$, and hence $(r_A, r_B) | (r_1, r_2)$. But $(r_1, r_2) = 1$, so $(r_A, r_B) = 1$; and therefore the pair (A,B) is distributive.

Since the pair (A,B) was chosen arbitrarily, M is a D-R-module.

To show necessity, assume that M is a D-R-module and show that every finite set of elements generates a cyclic module. Consider the elements $a, b \in M$. Then $H = Ra + Rb$ and H must be shown to be cyclic, i.e., there must be an element g such that $Rg = H = Ra + Rb$.

But H is a finitely generated module over R, a principal ideal domain. Thus by the fundamental theorem of finitely generated modules, either H is cyclic or $H = Rd_1 \oplus Rd_2$ where d_1, d_2 are nonzero elements in M and order $d_1 |$ order d_2. Now if H is cyclic, the proof is

completed. Therefore, assume H is not cyclic, hence $H = Rd_1 \oplus Rd_2$. Now $d_1, d_2 \in M$ implies Rd_1, Rd_2 is a distributive pair since M is a D-R-module. Hence by the lemma, for every $c \in Rd_1 \oplus Rd_2$ where $c \notin Rd_1$ or Rd_2, the relative orders of c with respect to Rd_1 and Rd_2 are relatively prime. Thus consider $c = d_1 + d_2$. Since $d_1, d_2 \neq 0$, $c \notin Rd_1$ and $c \notin Rd_2$. If, for example, $c \in Rd_1$, then d_2 would belong to Rd_1 and hence to $Rd_1 \cap Rd_2$. But $H = Rd_1 \oplus Rd_2$ implies $Rd_1 \cap Rd_2 = \{0\}$, so $d_2 = 0$ which is a contradiction. Thus $c \notin Rd_1$ or Rd_2 and there exists $r_1, r_2 \in R$, such that $r_1 c \in Rd_1$ and $r_2 c \in Rd_2$. Now $r_1 c = r_1 d_1 + r_1 d_2$, so $r_1 c \in Rd_1$ implies $r_1 d_2 \in Rd_1$, hence $r_1 d_2 \in Rd_1 \cap Rd_2$, and therefore $r_1 d_2 = 0$. Thus order $d_2 | r_1$. Similarly $r_2 d_1 \in Rd_2$, thus to $Rd_1 \cap Rd_2$, so $r_2 d_1 = 0$ and order $d_1 | r_2$. But since order $d_1 |$ order d_2, order $d_1 | r_1$ so order $d_1 | (r_1, r_2)$, and order $d_1 = 1$.

Then $1 \cdot d_1 = d_1 = 0$. But this is a contradiction since we assumed $d_1, d_2 \neq 0$. Thus H must be cyclic, hence $Ra + Rb$ is cyclic and then by induction every finite set of elements generates a cyclic module, so the necessity is proved.

The above theorem then leads to a rather strong result about finitely generated modules over principal ideal domains. For finitely generated modules, the theorem

says simply:

<u>COROLLARY</u>. <u>Let R be a principal ideal domain, and M a finitely generated R-module. Then M, a D-R-module, implies M is cyclic</u>.

<u>Proof</u>. If M is a D-R-module, then every finite set of elements generates a cyclic module. In particular, the finite generating set of M, generates a cyclic module, hence M is cyclic.

Thus if R is a principal ideal domain, the only finitely generated modules which are D-R-modules, are the cyclic ones.

<u>SECTION 3.</u> <u>COMPLEMENTATION CONDITIONS</u>.

If M is an R-module, in general $L_R(M)$ will not be complemented. For example, if M is any module with only one proper submodule, then $L_R(M)$ will not be complemented. This is not to imply, however, that $L_R(M)$ is not complemented only in rather trivial cases, or in cases where the lattice has "few" elements. Many lattices of submodules will have infinitely many elements and still will not be complemented.

<u>EXAMPLE</u>. Consider Z as a module over itself. Then rZ will be a submodule for every $r \in Z$. Then assume there exists a submodule A of Z such that A is the complement of rZ, i.e., $A \wedge rZ = \{0\}$ and $A \vee rZ = Z$. Now $A \vee rZ = Z$ implies there exists $a \in A$ and $rz \in rZ$ such that $a + rz = 1$. Then $rza \in A$ and $r(za) \in rZ$; since by assumption, A is a complement of rZ and $A \wedge rZ = \{0\}$, it must follow that $rza \in A\ rZ = \{0\}$. Thus $a \cdot a + rza = 1 \cdot a = a$ or $a \cdot a = a$. Since $a \in Z$, this implies $a = 0$ or $a = 1$. If $a = 1$, then $A = Z$, and therefore $A \wedge rZ = \{0\}$ implies $rZ = \{0\}$.

On the other hand, $a = 0$ implies $rz = 1$; so $rZ = Z$ and then again $A \wedge rZ = \{0\}$ implies $A = \{0\}$. Therefore it is seen that if rZ is a submodule of Z, which has a complement, either $rZ = Z$, or $rZ = \{0\}$. Thus, only in the trivial cases will a submodule of Z be complemented. In all nontrivial cases, i.e., A, a proper submodule of Z, $A \neq \{0\}$, there will not exist a complement for A.

Just as there are many cases where $L_R(M)$ is not complemented, there also are many interesting cases where $L_R(M)$ is complemented. If M is a vector space (hence a module), then M has a basis and $L_R(M)$ is complemented. The question is, how much of the "strength" of a vector space is needed in order to insure that the lattice

structure is complemented? Can the requirement that M be a vector space be loosened somewhat without losing the complementation of $L_R(M)$?

In finding a complement for a subspace of a vector space, much use is made of the fact that a vector space has a basis. This leads to the investigation of those modules which are not vector spaces, yet possess the same property, i.e., they have a basis.

First, a basis must be defined in a module context, then some of those modules which possess bases will be examined to see if their lattice structure of submodules is complemented.

In the following definitions, M will be an R-module, and U a set of elements of M.

<u>DEFINITION</u>. U <u>spans</u> M if for every element $m \in M$, there exists a finite subset of U, $u_1, u_2, \ldots, u_n$ and elements $r_1, r_2, \ldots, r_n \in R$ such that $M = r_1u_1 + r_2u_2 + \ldots + r_nu_n$.

<u>DEFINITION</u>. U is <u>linearly independent</u> if $r_1u_1 + r_2u_2 + \ldots + r_nu_n = 0$ where the u_i's are distinct elements of U, implies $r_i = 0$ for every i.

DEFINITION. If U is a linearly independent set which spans M, then U is said to be a basis for M.

DEFINITION. An R-module which possesses a base is said to be a free R-module.

Now a free module over the right kind of a ring is very close to a vector space. In vector spaces, the proof of complementation comes essentially from the fact that any subspace has a basis and that this basis can be extended to a basis of the vector space. The "nicest" thing to happen would be for a free module over a principal ideal domain to possess these properties, since this is the requirement which was put on the ring R in the theorems dealing with distributivity. Because finitely generated modules over principal ideal domains have nice structural properties, this class of structures would appear to have a chance at insuring that $L_R(M)$ be complemented since the following lemma would then apply.

LEMMA 1. *If R is a principal ideal domain, and M is any free R-module of finite type, then any submodule of M is a free module of finite type.*[1]

---

[1]S. MacLane and G. Birkhoff, *Algebra* (Toronto: The MacMillan Company, 1967), p. 358.

Unfortunately, the fact that M is a finitely generated, free module over a principal ideal domain, is not enough to insure that $L_R(M)$ will be a complemented lattice. The following example applies!

<u>EXAMPLE</u>. Let M be the module of all 2-tupules generated by (1,0), (0,1) over R the ring of integers with addition and scalar multiplication in the usual manner. R being the ring of integers implies R is a principal ideal domain. Let A be the submodule generated by (2,0). Obviously, this is a free module on one generator. There does not exist a B, submodule of M, such that $A \wedge B = \{0\}$ and $A \vee B = M$.

Assume that such a B exists and $A \wedge B = \{0\}$. Now B, a submodule of a free module over a P.I.D., implies B is free on a set of generators β where $\#\beta \leq 2$ = dimension of M. If $\#\beta = 2$, then $A \wedge B = \{0\}$ implies the generators of A and the generators of B must be linearly independent. Hence there exists three linearly independent elements in M, which contradicts the fact that the dimension of M is two. Therefore $\#\beta = 1$, or B is generated by one element. Now $A \vee B = M$ and $(1,0) \in M$ implies $(1,0) \in A\ B$ and so there exists $x, y \in Z$ so that $x(2,0) + y\,(h,k) = (1,0)$ where (h,k)

is the generator of B. Thus $(2x + yh, 0 \cdot x + yk) = (1,0)$ or $2x + yh = 1$, and $0 \cdot x + yk = 0$, i.e., $yk = 0$. Since R has no zero divisors, $yk = 0$ implies $y = 0$ or $k = 0$. $k = 0$ implies $(h,k) = (h,0)$ but then $h(2,0) - 2(h,0) = 0$ and either $h = 0$, in which case $B = \{0\}$ and $A \vee B = A \neq M$ and we have a contradiction, or $h \neq 0$ in which case $(h,0)$ and $(2,0)$ are not linearly independent and so $A \wedge B \neq \{0\}$, which also gives us a contradiction. Therefore, $y = 0$. But $y = 0$ implies $2x + yh = 2x = 1$ and since there is no $x \in Z$ such that $2x = 1$, it is clear that no such $x, y \in Z$ exists. Hence $(1,0) \notin A \vee B$ and so $A \vee B \neq M$, which implies A has no complement in M.

In fact, even if R is only an integral domain, if R_R is an R-module over itself such that $L_R(R)$ is a complemented lattice, a rather strong result can be reached about R. Knowing that R is an integral domain, $L_R(R)$ being complemented will force R to be a field.

<u>THEOREM V</u>. <u>Let R be an integral domain and R_R, R as a module over itself. Then the lattice $L_R(R)$ is complemented if and only if R is a field</u>.

<u>Proof</u>: If R is a field, then R_R is a vector space and clearly $L_R(R)$ is complemented, thus the sufficiency is proved.

To prove necessity, it must be shown that for every nonzero $a \in R$, there exists a multiplicative inverse of a in R. Consider any $a \in R$, $a \neq 0$. Then Ra is a submodule of R_R and hence is complemented in $L_R(R)$. Let B be this complement. Then $Ra \wedge B = \{0\}$ and $Ra \vee B = R_R$. Now for any $b \in B$, since $B \subseteq R$, $ba \in Ra$, and $a \in R$ implies $ab \in B$. R commutative, implies $ab \in Ra \wedge B$. But $Ra \wedge B = \{0\}$ and $a \neq 0$ by assumption. Then R an integral domain implies there are no zero divisors in R and so $b = 0$. Since b was chosen arbitrarily, this is true for every $b \in B$ and therefore $B = \{0\}$. Now $Ra \vee B = R_R$ implies $Ra = R_R$ and hence $1 \in Ra$. So there exists an element $a^{-1} \in R$ such that $a^{-1}a = 1$. Therefore, a has a multiplicative inverse for every $a \in R$, so R is a field.

Clearly then, requiring R to be a principal ideal domain is not enough. The problem is that while Lemma 1 insures the existence of a basis for every submodule of a properly chosen module, it does not imply that this basis can be extended to be a basis for the module. The following theorem establishes that this additional property is sufficient for $L_R(M)$ to be complemented.

THEOREM VI. *If M is an R-module, a sufficient condition for $L_R(M)$ to be complemented is that every submodule of M over R, has a basis which is extendable to be a basis for M.*

Proof: Consider A, a submodule of M. By assumption, A has a basis, say A_o, and this basis can be extended to be a basis for M. Call this extension M_o. Now let $B_o = M_o \setminus A_o$, and let B be the submodule generated by B_o. Now B is the complement of A. Consider $m \in A \wedge B$; this implies there exist finite sets $a_1, a_2, \ldots a_n \in A_o$ and $r_1, r_2, \ldots r_n \in R$ so that $m = r_1a_1 + r_2a_2 + \ldots + r_na_n$ and there exist finite sets $b_1, b_2, \ldots b_m \in B_o$ and $s_1, s_2, \ldots s_m \in R$ such that $m = s_1b_1 + s_2b_2 + \ldots + s_mb_m$ then $0 = m - m = r_1a_1 + r_2a_2 + \ldots + r_na_n + (-s_1)b_1 + (-s_2)b_2 + \ldots + (-s_m)b_m$. Now, that $a_1, a_2, \ldots a_n, b_1, b_2, \ldots b_m \in M_o$ and M_o linearly independent implies $r_1, r_2, \ldots r_n, s_1, s_2, \ldots s_m$ all equal to zero; so $m = 0$ and hence $A \wedge B = \{0\}$.

Since A_o spans A, B_o spans B, $A_o \cup B_o$ spans $A \vee B$, but $A_o \cup B_o = M_o$ and M_o spans M so $A_o \cup B_o$ spans M and therefore $A \vee B = M$. Thus B is the complement of A. Since A was any submodule of M, $L_R(M)$ is a complemented lattice.

Therefore it has been established, that if given any submodule, not only does that submodule have a basis, but that basis can be extended to be a basis of the module, then the lattice of all submodules of that module will be complemented. This condition is not a necessary one, however, as the following example shows.

EXAMPLE. If F_1, F_2 are fields, let $R = F_1 \oplus F_2$. R is a ring. Use addition and scalar multiplication by components and R is a module over itself. Now the submodules or R will be exactly the ideals of R. But the only ideals of R, are R, $\{(0,0)\}$, $F_1 \oplus \{0\}$ and $\{0\} \oplus F_2$, and $L_R(R)$ is complemented; R and $\{(0,0)\}$ the zero element are complements in any lattice. Now consider $(F_1 \oplus \{0\}) \wedge (\{0\} \oplus F_2)$, if (a,b) is an ordered pair in the meet, then $(a,b) \in (F_1 \oplus \{0\})$ implies $b = 0$ and $(a,b) \in (\{0\} \oplus F_2)$ implies $a = 0$, so $(a,b) = (0,0)$ or $(F_1 \oplus \{0\}) \wedge (\{0\} \oplus F_2) = (0,0)$. If $(a,b) \in R$ that implies $a \in F_1$, $b \in F_2$, so (a,b) can be written as $(a,0) + (0,b)$ where $(a,0) \in F_1 \oplus \{0\}$ and $(0,b) \in \{0\} \oplus F_2$ so $(a,b) \in (F_1 \oplus \{0\}) \vee (\{0\} \oplus F_2)$ and therefore $(F_1 \oplus \{0\}) \vee (\{0\} \oplus F_2) = R$ and thus they are complements. So $L_R(R)$ is a complemented lattice. But the submodules of R_R do not all have a basis. Consider $F_1 \oplus \{0\}$. If $(a,0) \neq 0$ is a basis element of $F_1 \oplus \{0\}$ $(0,1)(a,0) = (0,0)$ and $(0,0)(a,0) = (0,0)$; so $(0,0) \in (F_1 \oplus \{0\})$ but

it has no unique representation in terms of basis elements. Since this is true, $F_1 \oplus \{0\}$ must not have a basis.

The problem now becomes finding a module with the properties required by Theorem VI. Since a principal ideal domain lacks only multiplicative inverses to be a field, and yet R being a P.I.D. is not sufficient, requiring that R be a division ring is an obvious next step. In the following lemma and its corollary, it is established that if D is a division ring, and if M is a D-module, then every submodule of M has a basis which can be extended to be a basis of M.

<u>LEMMA 2.</u> <u>If M is a module over D, a division ring, and A_o is any linearly independent set in M, then A_o can be extended to be a basis for M.</u>

<u>Proof</u>: Consider $\Gamma = \{A \mid A$ is a linearly independent subset of M, $A_o \subseteq A\}$. Let $\mathbb{C}$ be a chain in Γ, that is if $A, B \in C$ then either $A \leq B$ or $B \leq A$. If $E = \bigcup_{A \in \mathbb{C}} A$; then E is a linearly independent subset of M. For if F is any finite subset of E and $F = \{m_1, m_2, \ldots, m_n\}$ then there exists $A_1, A_2, \ldots A_n$ in C such that $m_1 \in A_1$, $m_2 \in A_2$, ... $m_n \in A_n$. Since C is a chain, $A_1 \cup A_2 \cup \ldots \cup A_n$ is one of the sets $A_1, A_2, \ldots A_n$. Since

all the A_i's are linearly independent, and $F \subseteq A_1 \cup A_2 \cup \ldots \cup A_n$, F is a subset of a linearly independent set and hence linearly independent. Since E contains every A in the chain $\mathbb{C}$, and E is linearly independent, E is an upper bound for $\mathbb{C}$. Thus by Zorn's Lemma, there exists a maximal linearly independent subset in M which contains A_o. Call this maximal set, M_o. Now M_o spans M. To establish this, consider any $x \in M$. If x does not belong to the span of M_o, then that implies that $\{x\} \cup M_o$ is a linearly independent set. If not, there exists $m_1, m_2, \ldots m_n \in M_o$, and $d_o, d_1, d_2, \ldots d_n \in D$ such that $d_o x + d_1 m_1 + d_2 m_2 + \ldots + d_n m_n = 0$ and not all d_i's are zero. Now if $d_o = 0$, all the other d_i's must be zero since $m_1, \ldots m_n$ is a linearly independent set. Since we assumed not all d_i's are zero, $d_o \neq 0$. Then since D is a division ring, there exists $d_o^{-1} \in D$. Then

$$x = (d_o^{-1} d_o)x = (-d_o^{-1} d_1)m_1 + (-d_o^{-1} d_2)m2 + \ldots + (-d_o^{-1} d_n)m_n$$

which implies x belongs to span of M_o. Since we assumed this is not true, $\{x\} \cup M_o$ must be linearly independent. But this is a contradiction since by Zorn's Lemma we know

that M_o is a maximal linearly independent set. Hence x must belong to the span of M_o for every $x \in M$, so M_o spans M. Therefore M_o is a linearly independent spanning set of M, and hence M_o is a basis for M, and contains A_o, so the lemma is proved.

COROLLARY. If M is a module over D, a division ring, then M is a free module.

Proof: Follows immediately from the lemma. Let $A_o = \emptyset$, then A_o is a linearly independent subset of M and hence can be extended to be a basis for M. Therefore, M has a basis and so it is a free module.

This then, establishes that if M is a module over a division ring, then M satisfies the requirements of Theorem VI and hence $L_D(M)$ is a complemented lattice. This fact is stated in the following theorem.

THEOREM VII. If M is a module over D, a division ring, then $L_D(M)$ is a complemented lattice.

Proof: Consider A any submodule of M. A is obviously a module over a division ring, hence by the corollary, a free module with a basis A_o. By the lemma, A_o can be extended to be a basis for M, so any submodule of M has a

basis which can be extended to be a basis for M. Hence by Theorem VI $L_D(M)$ is a complemented lattice. Thus if M is any module over a division ring, L(M) is a complemented lattice.

This corollary then, easily follows.

COROLLARY. *If M is a module over a division ring D, then $L_D(M)$ is relatively complemented.*

Proof: From the preceeding theorem, $L_D(M)$ is complemented. Earlier, we saw that $L_D(M)$ is always modular. Then $L_D(M)$, a modular, complemented lattice, implies $L_D(M)$ is relatively complemented.

Note, however, that this does not imply that any of these complements are unique. Consider any arbitrary vector space V. Clearly, it satisfies the requirements to form a complemented lattice L(V). But it was earlier seen that if the space V is of dimension two or more, L(V) will not be distributive.

By the "Birkhoff Distributivity Criterion,"[1] a lattice is distributive if and only if no interval [a,b]

---

[1]G. Szasz, *Introduction to Lattice Theory*, 3rd. Ed. (Academic Press, New York - London, 1963), p. 90.

of the lattice includes an element having two different relative complements in [a,b].

Thus L(V) not distributive implies that there are intervals [a,b] in L(V) which have two different relative complements.

SECTION 4. A Covering Condition.

DEFINITION. If a,b are elements of a lattice such that $a < b$, and there is no element x, such that $a < x < b$, then it is said that a is covered by b. This will be expressed by the symbol $a \prec b$.

If M is an R-module, in general, elements of $L_R(M)$ will not be covered. An obvious example is to again consider the ring of integers as a module over itself. In the lattice of submodules of this module, the null element {0} will have no covering element. Since Z is a principal ideal domain, here again R being a P.I.D. is not sufficient to assure that $L_R(M)$ will have the desired properties. It is clear, however, that the modules discussed in the previous section, i.e. modules over division ring, would have lattices of submodules where every element had a cover. Here again the ability to get a basis for M, and

the availability of multiplicative inverses, is enough to insure the presence of covering elements.

<u>THEOREM VIII</u>. <u>If M is a module over a division ring D, and $A \in L_D(M)$, where $A \neq M$, then there exists $B \in L_D(M)$ such that $A \prec B$.</u>

<u>Proof</u>: If $A \neq M$ and $m_1, m_2, \ldots m_n$ is a basis for M, then there exists an m_j such that $m_j \notin A$. Then if we let $B = A \vee Dm_j$, B is a cover for A. Consider C such that $A \lneq C \leq B$. $A < C$ implies there exists a $c \in C$ such that $c \notin A$. Then $c \in C \leq B$ implies $c = a + dm_j$ for some $a \in A$. D, a division ring, implies $d^{-1} \in D$ thus $m_j = (d^{-1})c + (-d^{-1})a$. But $a \in A < C$ and $c \in C$ so $m_j \in C$. Thus $B = A \vee Dm_j \leq C$ and we have $B = C$.

B I B L I O G R A P H Y

Baer, R. "The Significance of the System of Subgroups for the Structure of the Group," Amer. J. Math. 61. (1939), pp. 1-44.

Birkhoff, G. Lattice Theory, American Math. Soc. Colloquium Publ. 25, revised edition, New York, 1948.

Kaplansky, I. Commutative Rings, Allyn and Bacon, Inc., Boston, 1970.

Lambek, J. Lectures on Rings and Modules, Blaisdell Publishing Company, Waltham-Toronto-London, 1966.

MacLane, S. and G. Birkhoff. Algebra, The MacMillan Company, Toronto, 1967.

Northcott, D. Lessons on Rings and Modules and Multiplicities, The University Press, Cambridge, 1968.

Ore, O. Structures and Group Theory, II, Duke Math. J. 4. (1938), pp. 247-269.

Suzuki, M. "Structure of a Group and the Structure of Its Lattice of Subgroups," Ergebnisse der Math. U. ihrer Grenzgeb. New series 10 Springer-Verlag, Berlin-Gottingen-Heidelberg, 1956.

Szasz, G. Introduction to Lattice Theory. 3rd Ed. Academic Press, New York-London, 1963.

V I T A

Gary Dean Jensen was born in Hallock, Minnesota, on July 18, 1946, the son of Mr. and Mrs. Melvin R. Jensen. After graduation from St. Thomas Military Academy, St. Paul, Minnesota, in 1964, he entered the United States Naval Academy in Annapolis, Maryland. While a senior at the Naval Academy, he was selected for the "Junior Line Officer Scientific Education (BURKE) Program." Under this program, he was scheduled to have two years of sea duty following graduation from the Naval Academy, and would then attend a civilian university for postgraduate work. In June, 1968, he received a Bachelor of Science degree from the Naval Academy, and a commission as an Ensign in the United States Navy. After completion of Naval Submarine School in New London, Connecticut, he was assigned to a submarine stationed in Pearl Harbor, Hawaii. Upon qualification in submarines, Lt. Jensen entered the Graduate School of The University of Texas in September, 1970.

Permanent address: 2134 Summit Avenue
St. Paul, Minnesota

Thesis
J4727

135175

Jensen

Some lattice theoretic theorems concerning the submodules of a module.